# Transcript

## Section A

00:00:00 Interviewer

Next, we are going to conduct an interview with TPR3.

00:00:07 Interviewer

Let's start with Section A. The first question should be about… you work in a private network security, right?

00:00:13 TPR3

Yes, I work for a private network security provider.

00:00:16 Interviewer

The second question is how long have you worked in this unit? Oh, sorry, which unit do you work in?

00:00:24 TPR3

Currently, I work at [a private company].

00:00:28 TPR3

I've been here for almost two years. My previous job was at the [the name of a corporate foundation], which is a corporate foundation and a government think tank. I worked there for nine years.

00:00:46 Interviewer

Wow, that's a long time.

00:00:49 TPR3

Yes, and in both of these positions, my title is director.

00:00:54 TPR3

But the director position in the foundation is different from that in a private enterprise. In the foundation, the director is equivalent to a department head, while in a private enterprise, it's more like a team leader.

00:01:14 Interviewer

Okay, let's move on to the fourth question. What is your current role in this position?

00:01:21 TPR3

Currently, our main focus is on providing cybersecurity protection services. So, when our clients encounter cybersecurity incidents or face issues with our cybersecurity products, or even encounter technical problems related to cybersecurity or IP, our department is available to assist them.

00:01:29 Interviewer

OK.

## Section E

00:01:45 Interviewer

So now you have answered questions four and five, because the fourth question is about you being a director. Okay, now we will move on to Part E, which is on the next page.

00:01:57 Interviewer

Yes, that's right, because Part B is about the interviewing police officer.

00:02:02 TPR3

OK.

00:02:04 Interviewer

For Part E, the first question I want to ask is about your experience. What do you think are the main network attacks that Taiwan is facing now? And what are the methods of attack? Can you give examples to illustrate?

00:02:17 TPR3

Okay, first of all, there are two issues I want to share with you. The first part is about the target of the attack in Taiwan. We should first understand who is interested in us. According to the data I have on hand, 80% of the attacks on Taiwan last year came from across the strait (China). As for why this cross-strait accounts for 80%, and how the information is verified, this part may not be convenient to disclose, but we have relevant information in hand. Under such circumstances, the network attacks against Taiwan, whether to private or government units, generally fall into two categories. The first is the theft of sensitive information or trade secrets, and the second is further extortion, which is a common practice. For example, recently we helped a high-tech manufacturer who was attacked by hackers. The main reason was the leakage of their business data related to their products. The reason for the leakage was that they were being extorted by hackers. The hacker family and the tool used by the hacker in this attack are commonly referred to as LockBit.

00:03:55 Interviewer

OK.

00:04:03 Interviewer

OK, then we move on to the second question. According to your experience, what do you think is the main target of network attacks in Taiwan now? In other words, why are these targets becoming the targets of network attacks?

00:04:23 TPR3

Well, the targets of network attacks are mainly divided into two stages.

00:04:26 Interviewer

I see.

00:04:27 TPR3

The first stage is called pre-attack preparation, and the most common target for this stage is IoT devices. Why is IoT device a pre-attack preparation? Because after being attacked, it can become a hacker's springboard, or it can hide some tools there. Since IoT devices are usually not easy to be protected, they are the favorite target of hackers. This is the pre-attack preparation stage.

00:04:57 TPR3

During the actual attack, hackers may use a series of methods. Generally, the main target is sensitive information of enterprises, as mentioned earlier. The theft of sensitive information from enterprises is usually supported by so-called "internet armies" because they have specific goals.

00:05:19 TPR3

The so-called "internet armies" refer to, for example, the Chinese-supported hacker group. This hacker group may receive instructions from the government and needs to steal specific technologies. At this time, it is a target. The second most common target is because hackers need to survive, and now their division of labor is very detailed.

00:05:45 TPR3

They used to be able to do everything themselves, but now it is a group of people, and each person is responsible for a stage. These hackers used to pursue personal achievements in the past, but now they pursue a career. Therefore, they have a need for economic income, and the easiest way to obtain economic income is through extortion. Therefore, in terms of extortion, everything is possible as long as they think that your company assets are valuable, and this value goes beyond the actual loss of money and affects the reputation. These are all targets that they will be interested in.

00:06:34 Interviewer

Okay.

00:06:35 Interviewer

Well, I would like to further ask, do you think there are any specific industries that are more vulnerable to attacks?

00:06:43 TPR3

The three common ones in Taiwan are government, finance, and high-tech.

00:06:48 Interviewer

Government, finance, and high-tech.

00:06:51 Interviewer

So, what do you think is the reason?

00:06:54 TPR3

Oh, it's definitely a bit of a declarative tone when it comes to attacking government agencies.

00:07:00 TPR3

Um, yes, I have the ability to further influence government agencies like you, and that has a bit of a declarative tone. As for finance, they actually need to know some sensitive information, such as personal data, because many Taiwanese investors, including individual investors like us, are involved in financial investment. Therefore, the financial department will have a lot of personal information stored, and the second part is actually a hypothetical issue, the so-called hypothetical issue is this.

00:07:42 TPR3

When you want to influence the operations of a country, targeting the financial market is the easiest way. Under the premise of affecting the financial market, one needs to conduct training exercises. This training involves attempting attacks on various entities, such as brokerage firms, to assess their effectiveness. If these attacks prove to be successful, they can serve as a blueprint for future invasions of the country.

00:08:10 TPR3

So, during this training process, they need to find real targets. This is commonly seen in cases where certain banks or brokerage firms are attacked. However, as Taiwan's cybersecurity capabilities are becoming stronger due to government emphasis and regulations, private enterprises are also increasing their budgets and resource allocation for cybersecurity. This could be related to the subsequent discussion, where the impact of such measures may lead to businesses believing they have sufficient security measures in place. Consequently, hackers may shift their targets away from specific companies and instead focus on their upstream and downstream connections. This is related to the further development and planning of government-company collaboration and policies that you mentioned later.

00:09:20 Interviewer

Okay, thank you, so let's move on to the third question.

00:09:25 Interviewer

So, the third question is, what do you think are the main factors affecting Taiwan's internet security?

00:09:32 TPR3

Actually, the main factor now is the geopolitical issue, yes, the geopolitical issue, which is more critical. If we didn't have this issue, then of course, Taiwan's supply chain security is also critical. The so-called supply chain, after all, many Taiwanese companies are doing OEM for international giants.

00:09:55 TPR3

These trade secrets, combined with trade methods, lead to certain countries not being able to obtain certain technologies. This kind of thing will have an impact on specific countries, so there is a need to steal commercial secrets. So, geopolitical issues and technological developments will both be very important reasons for Taiwan's internet security impact.

00:10:21 Interviewer

Okay, I see.

## Section F

00:10:23 Interviewer

Alright, let's move on to part F. The first question in part F is about the technologies and services that your company currently provides in terms of cybersecurity.

00:10:38 TPR3

[A private company] provides endpoint protection services and supplies intelligence to our customers. So we provide our customers with protection on all their endpoints, including tools for defense and our assistance with monitoring and response. These are our main technologies and services.

00:11:05 Interviewer

OK.

00:11:10 Interviewer

Now, for the second question, what are your main sources of customers?

00:11:14 TPR3

Actually, we have clients from most industries in Taiwan.

00:11:20 TPR3

To name a few, we serve the government, high-tech, finance, transportation, e-commerce, education, telecommunications, and network industries.

00:11:45 Interviewer

So, you have clients from most industries in Taiwan?

00:11:46 TPR3

Yes, mostly larger-sized enterprises. To be more specific, we cover clients in the medium to large enterprise size range, as they are the ones who typically require our services. However, small and medium-sized enterprises may not necessarily need it. So, in general, our customer base includes medium to large-sized enterprises.

00:12:09

OK.

00:12:10 Interviewer

So, small and medium-sized enterprises may not necessarily want it because of their limited budget, right?

00:12:15 TPR3

Aside from budget and regulatory requirements, companies are primarily focused on survival, and cybersecurity is a risk consideration. Why would they say they don't need it? It's simple: if the losses from the situation are controllable and lower than the investment, they would rather take the loss.

00:12:36 Interviewer

I see, understood.

00:12:40 Interviewer

Moving on to the third question, what are the main reasons why these customers you mentioned usually seek your services?

00:12:49 TPR3

Actually, there are only two main reasons. The first is government regulatory requirements, which are important not only for protecting businesses but also for some of the government's future development strategies. We can discuss this later. The second is the actual defense needs, and the reasons for this were mentioned earlier: the first concern is geopolitical, and the second one is about their involvement in assisting large enterprises with manufacturing and design, where confidentiality is of utmost importance.

00:13:26 Interviewer

May I ask another question? Do these customers who seek your services usually come to you before any front-end events occur, or is it usually after they have been attacked?

00:13:42 TPR3

You asked a great question! In the past, it was mostly the latter scenario. Before the government's regulation requiring all listed companies to establish a Chief Information Security Officer (CISO) position, companies often viewed cybersecurity as an expense to be minimized. They would only seek cybersecurity services after experiencing severe incidents that were beyond their control. Therefore, there are two key factors: first, an incident needs to occur, and second, the incident should be beyond the company's control. If the incident is controllable, they are less likely to seek assistance from service providers.

00:14:50 Interviewer

So this is before the regulatory requirements were established?

00:14:52 TPR3

Yes.

00:14:54 Interviewer

I think this concept is somewhat similar to insurance, right?

00:14:57 TPR3

Yes, that's right, it's very much like insurance.

00:14:59 Interviewer

Yes, because you may invest in insurance, but you may not actually use it, so you might feel like it's a waste of money.

00:15:22 TPR3

Yes, but now, cybersecurity has put this concept into the minds of business owners, so to some extent, it's actually a part of risk management. It's a part of management, not just a cost.

00:15:43 Interviewer

OK, so let's move on to the fourth question. Most of your clients come to you seeking help with a specific aspect of cybersecurity that they lack or are deficient in. Which part do you think they're particularly lacking in or unaware of?

00:16:02 TPR3

You hit the nail on the head: it's the lack of security awareness.

00:16:05 Interviewer

I see.

00:16:07 TPR3

In addition to the lack of security awareness, there is also a problem with their self-awareness. They don't even know what they're missing.

00:16:12 Interviewer

Uh-huh.

00:16:16 TPR3

This is a big problem because if you don't even know what you're missing, you naturally don't know who to turn to for help.

00:16:24 TPR3

In addition, I think another key issue is their lack of professional knowledge related to cybersecurity. If they don't have this knowledge, it will be related to the problems mentioned earlier, because without this background, they won't even know their own needs.

00:16:44 Interviewer

So basically, within companies, there may be a shortage of talent, including information security personnel, and the company may not value it as much?

00:16:55 TPR3

Yes, this is a big problem.

00:17:00 Interviewer

So, the government may need to strengthen some education and training, or?

00:17:06 TPR3

Uh, talent cultivation is key. Yes, talent cultivation is key. Apart from that, currently, since the Republic of China calendar, can I use the Republic of China calendar? From the 106th (2017) to 107th (2018) year, the government has proposed a concept called "information security is national security."

00:17:18 Interviewer

Yes, yes, yes.

00:17:28 TPR3

The concept of "information security is national security" actually has two purposes. The first purpose is to raise the level of information security issues from the government's perspective, and the second purpose is to let all people, including civilians and companies, pay attention to it. Because this kind of thing takes time to develop and to build the concept into people's minds, so that everyone knows that this has become a norm, right?

00:17:58 Interviewer

Okay, great.

00:18:00 Interviewer

Then I'll move on to the fifth question. What are the main types of network attacks that you are deaTPR3g with now?

00:18:14 TPR3

Before I answer the question, oh, I want to share my thoughts with you first, which is that I think this series of questions 56789 is poorly designed.

00:18:23 Interviewer

Uh, it's okay.

00:18:25 TPR3

And do you know why?

00:18:28 TPR3

For example, if we take the fifth question as an example and you ask about forms of network attacks, strictly speaking, I roughly understand the angle from which you want to ask the question. For instance, networks are a level, servers are another level, and end points are yet another level. So from these different levels, what is your scope of responsibility? Maybe you want to make this kind of classification. But the reason I say they are poorly designed is….

00:18:59 TPR3

Basically, when we look at problems, I'm not talking about research angle, but from the perspective of dealing with problems and events, we don't just look at one point, we must cover a range of aspects. So if we want to deal with this type of attack, we must cover all aspects. We must consider network problems, server problems, configuration problems, and a series of other issues. Therefore, let me answer your question from a different angle.

00:19:29 TPR3

Looking at it from a different angle, we should look at the attack lifecycle, from the initial stage to the final stage when the attack is successfully completed. There are roughly five stages, and we divide them into three categories: before, during, and after the event. Have you heard of this before?

00:20:00 Interviewer

Actually, my question is similar, I wanted to ask something like this, yes.

00:20:03 TPR3

Our main focus is on the during stage, which is where our defense range lies. Why do I say this? Because our concept is that all protection, barriers, and firewalls will eventually be breached. So when it is breached, what we need to deal with is how to respond. How do we discover it in the first place, and how do we mitigate it as soon as possible?

00:20:30 TPR3

This is our defensive concept and spirit. So regarding this question, our objective and defense are mainly aimed at the investigation, response, and root cause analysis after the hacker invasion attack is successful. This is the scope we are dealing with, right?

00:20:52 Interviewer

Yes, actually this is what I wanted to ask, because I read a lot of literature, and some books mention that many of the preparations beforehand are sufficient. However, for example, many of the antivirus software on the market or some strategies are not able to respond once the defense line is breached.

00:21:12 TPR3

Yes, that's right.

00:21:13 Interviewer

So you set the wall very high, but you didn't think about that wall.

00:21:18 TPR3

There is a possibility of being breached.

00:21:19 Interviewer

Yes, so it becomes that once you are breached, you are completely paralyzed. So that is what I really want to ask, if your company is doing anything special in this area?

00:21:28 TPR3

Yes, we focus on this area.

00:21:28 Interviewer

Okay, that's great, so I hope you can share more about this area.

00:21:35 TPR3

Let me give you another technical term to remember: cyber defense matrix. Cyber defense matrix is a framework that is very popular and applicable in our field. It has two dimensions: the time axis, which refers to different stages, and the protection surface, which refers to different defense areas. By combining different stages and defense areas, we can create a cyber defense matrix.

00:22:14 Interviewer

So, the stages are basically the ones you mentioned earlier, before, during, and after?

00:22:17 TPR3

Yes, roughly categorized as before, during, and after.

00:22:19 Interviewer

Okay.

00:22:20 Interviewer

And what about the defense areas?

00:22:22 TPR3

The defense areas refer to different technical methods, such as network, endpoint, data, server, and encryption. It has a vertical axis with a series of technical methods for defense.

00:22:41 Interviewer

OK.

00:22:42 Interviewer

What was it called again?

00:22:44 TPR3

Cyber defense matrix.

00:22:46 Interviewer

And you said the defense areas are the protection surfaces?

00:22:49 TPR3

Yes, the defensive techniques.

00:22:51 Interviewer

OK.

00:22:52 TPR3

The vertical axis represents the defensive techniques, and the horizontal axis represents the stages.

00:22:55 Interviewer

Okay, so you guys analyze by using that kind of matrix?

00:23:04 TPR3

Yes, that's right.

00:23:07 Interviewer

Then, for the sixth question, how do you think you should answer? Like, after breaking through the defense, how do you guys handle it? What would be the general approach?

00:23:27 TPR3

In this part, there's only a key point conceptually, which is speed comparison.

00:23:30 TPR3

Okay, so how do we compare speed? The first thing is, can you grasp what's happening in the first moment? The second thing is, once you know what's happening, how do you, um, do the damage control? Let me give you an example. For example, an enterprise's firewall is a lot like a dam.

00:23:59 TPR3

The dam may collapse due to various factors. When it collapses, does water rush down from the top?

00:24:06 TPR3

In this situation, how do you protect the village below? The first thing is that you need to find a way to be aware of the situation as quickly as possible. You need to know when the dam starts leaking, you can't wait until the dam completely collapses before you realize it. So the first thing is to save time. The second thing is that when the water is rushing down, you must take a series of actions to divert the water to another place or create other barriers, or evacuate people. This is called emergency response. OK, and emergency response is also about saving time. That is, I have completed the emergency response before it causes damage. So detection and emergency response are the two key points in this question, right.

00:24:37 Interviewer

Yeah, I see.

00:24:54 TPR3

The two key technologies are detection and emergency response.

00:24:56 Interviewer

Detection and emergency response.

00:24:57 Interviewer

Okay.

00:25:02 Interviewer

So now we move on to the seventh question. Is the seventh question not well phrased? Because what I want to ask is, with the technology you provide, because you just mentioned detection and response, I think response is a bit like the concept of network resilience. It's like if a company suddenly loses power, you may have backup power so that your company can continue to operate and not be completely without power. So I think the concept of network resilience is a bit like this.

00:25:34 TPR3

Well, I would describe network resilience with another word, which is "resilience." (Here is the matter of translation)

00:25:43 Interviewer

Ah, yes, in English it's "resilience."

00:25:47 TPR3

Yes, resilience for us is still a post-event concept, not during the event. Of course, it's not entirely incorrect. In the context of resilience, let me explain from a different perspective. As you mentioned earlier, if your company's power supply is disrupted, you need a backup power source to support its continuous operation. However, resilience and response are different concepts. Response is more like when my data is being stolen by a hacker. During the theft process, let's say we're watching a movie, and there's a progress bar indicating the percentage. I need to cut off the connection before it completes. If I cut it off early, it means the hacker has stolen only a small portion. If I cut it off later, it means the hacker has stolen a significant amount. If the progress bar reaches 100%, it means the hacker has stolen all my data. Therefore, in the response phase, we strive to intervene at a specific percentage to minimize the damage. This concept is not exactly the same as resilience.

00:26:45 Interviewer

So then in terms of the concept of resilience, do you have something that you can share?

00:26:51 TPR3

The resilience aspect, in my opinion, will focus on the so-called enterprise's cybersecurity management strategy. The reason is that within the enterprise, we should have a well-defined cybersecurity defense plan. This plan should include the organization's policies, such as the policy of being absolutely immune to hacker attacks - this is the strategic aspect. In response to these strategic aspects, you need to have a management mechanism. This means you should have daily tasks that involve checking all the defense measures and ensuring no signs of hacker intrusion - this is the management aspect. The technical aspect needs to align with the objectives set by the management aspect. Only with this series of cybersecurity planning can you ensure resilience. Without it, resilience is not achievable. Let me put it from another perspective. For instance, if I want to ensure that my online services are available 24/7 without interruption, it requires having backup power. Otherwise, my servers might experience power outage. So, in this case, the 24/7 availability is the policy objective. The second step is to regularly check the functionality of the backup power generators and conduct appropriate drills. This requires investing in a reliable power generator system. This example illustrates the integration of policy management and technical aspects.

00:28:21 TPR3

Therefore, in terms of resilience, it should be evaluated from the cybersecurity protection strategy of the entire organization.

00:28:30 Interviewer

So, it goes back to the fact that the enterprise itself must have such awareness in order to make a comprehensive plan?

00:28:33 TPR3

Yes, that's right.

00:28:34 TPR3

Yes, you need to have that kind of awareness.

00:28:40 Interviewer

Okay, the eighth and ninth questions can be answered together. Do you think there is any part of the technology services you currently provide that is inadequate, and you can improve it in the future?

00:28:54 TPR3

Well, to be honest, I think these two questions are not well designed because generally, no one will say that they are not good themselves.

00:29:08 Interviewer

Maybe the questions are too straightforward.

00:29:09 TPR3

But I can still answer this question, which is, um, I think a more appropriate way to put it is that…

00:29:16 TPR3

We should focus on our defensive range. However, the defensive range is limited. The protection area you cover is so large, but I cannot protect everything. I can only focus on this defensive range. If we use the three coverage areas of pre-event, during event, and post-event that we just talked about, and we only focus on the during event, what about before and after the event? We must have some professional vendors to cooperate with, and this is the only way to be effective, to complete the overall protection of the enterprise and meet its needs.

00:29:50 TPR3

So for the eighth and ninth questions, I think my answer would be that, first, it's not that we are insufficient, but that we will focus on our defensive range.

00:29:59 TPR3

And we are very confident that the enterprise can be very safe and secure within our defensive range. Where is the inadequacy? The inadequacy is from the perspective of the enterprise, not ours. The enterprise should find other solutions for the areas that they still need coverage but are not provided by us.

00:30:19 Interviewer

Okay, understood.

00:30:22 Interviewer

So, let's move on to the tenth question. I want to ask if your company has any plans to improve and enhance the services you provide in terms of the technology or services you offer? Or perhaps you could elaborate on the shortcomings of the companies you just mentioned?

00:30:41 TPR3

From my perspective, maybe not from the company's perspective, my perspective comes from some observations and influences that I had while cooperating with Israel.

00:30:53 Interviewer

Cooperating with Israel?

00:30:54 TPR3

Yes, because I have worked with Israel in my previous company.

00:30:58 TPR3

Their concept is like this: when they want to do something, they do it and they strive to be the best in the world, to the point where even big companies want to hire them. I think this is the right way to do it.

00:31:13 TPR3

I don't need to be able to do everything. I only aim to excel and be the best at what I do. So, in essence, for question 10, I prefer to emphasize our focus on detection and response. Ensuring that our detection and response capabilities are continuously up-to-date is crucial because hackers' attack methods are constantly evolving, and we must keep up with these advancements. Apart from that, we also need to be able to accelerate our actions. As mentioned in the previous example, we need to swiftly identify issues and promptly assist our clients in responding to them. This will be an area where we need to continuously improve both in terms of technology and service in the future.

00:31:56 Interviewer

OK.

## Section G

00:31:58 Interviewer

So now we are moving on to the G section. For the first question in the G section, I want to ask your personal opinion on the concept of cooperation between public government agencies and private sectors like yours in terms of internet security. Do you think this concept is helpful for the development of internet security?

00:32:16 TPR3

Um, I used to work in the company's joint defense department.

00:32:18 TPR3

In my previous job, I was in charge of company joint defense.

00:32:20 TPR3

I am familiar with this concept, um.

00:32:21 Interviewer

Okay.

00:32:23 TPR3

I would like to express that I have a positive view and attitude towards this idea and vision. I believe it is the right approach. The reason is that private entities possess information that is different from what the government has, and vice versa. Their information sets often do not overlap; instead, they could form a union of information.

00:32:44 TPR3

So, if you want to do information security well, the union of information will definitely be better than the intersection. Yes, so, in my personal opinion, the cooperation between the public and private sectors will definitely help improve the protection ability of enterprises and make government policy decisions more accurate.

00:33:05 Interviewer

In other words, the government may have the power to make decisions that can help us, but they may not have enough information from?

00:33:11 TPR3

Right, if they do not have enough information from the private sector, their decisions may be wrong.

00:33:16 Interviewer

So, let's move on to the second question. I would like to ask, according to your understanding, do you know if there are any public-private cooperation in Taiwan in terms of cybersecurity?

00:33:25 TPR3

The first and most mature mechanism is the Information Sharing and Analysis Center (ISAC).

00:33:44 Interviewer

OK, it's called ISAC?

00:33:50 TPR3

Yes, ISAC, this is the first mature mechanism. The second mature mechanism is the Computer Emergency Response Team (CERT).

00:34:07 Interviewer

CERT?

00:34:08 Interviewer

I can search a bit about CERT later.

00:34:10 TPR3

Yes, CERT.

00:34:14 Interviewer

I think I know about it. I might have seen it before.

00:34:17 TPR3

These two are quite popular and mature mechanisms. What are they doing? The first thing ISAC is doing is information sharing. The purpose of information sharing is to, for example...

00:34:21 Interviewer

OK.

00:34:31 TPR3

Company A is under attack. Can I share the patterns and techniques of the attack to industries related to me? Will this prevent secondary attacks on the related industries? Information sharing is the essence of this idea in the private sector. What about the public sector? After obtaining this information, can they use it to assist in formulating relevant policy objectives? For example, if they discover that the attacks aim to steal sensitive data from a specific company, they can establish a policy requiring encryption of all sensitive data related to the industry and conduct regular inspections. With this information, the government can tailor its policies accordingly. However, although there are benefits to such information sharing, it is challenging to implement in practice because companies are generally hesitant to disclose their security incidents due to reputation concerns.

00:35:30 TPR3

So how do you know if I don't tell you? I'll just wait for you to be attacked and then laugh at you, haha.

00:35:36 Interviewer

What if it's anonymous?

00:35:38 TPR3

Anonymity is important. Currently, the government has established the ISAC (Information Sharing and Analysis Center) with a mechanism that allows for anonymous reporting. However, it is unfortunate that the ISAC currently only covers critical infrastructure and some key enterprises related to government operations, such as those in the electricity, water, and transportation sectors. Companies like TSMC, despite being significant players like Taiwan Silicon Shield, are not included in the protection scope. There are two reasons for this. Firstly, TSMC may feel confident in their own capabilities and might not see the need for external assistance. Secondly, if TSMC were to establish a group and share their experiences with their upstream and downstream partners, it could create a more robust and effective system.

00:36:29 TPR3

But to do these things, it takes costs, and then it comes down to whether it's worth doing. The value of this information is difficult to assess, and it's not easy to evaluate its benefits. For companies, the most important thing is to see the benefits and effects.

00:36:43 TPR3

Under the premise of being difficult to measure, they may not be willing to initiate such a thing on their own.

00:36:47 Interviewer

So, maybe his cooperation may not be very good? Okay, then let's move on to the third question. Maybe we talked a little bit about it earlier, but I want to ask you what your thoughts are on these cooperation mechanisms? And also, are there any more difficult points that you think are worth mentioning regarding such public-private collaborations?

00:37:06 TPR3

OK, the operational mechanism I mentioned just now is helpful in the short term from the perspective of the country or a unit.

00:37:14 TPR3

The so-called short-term assistance means that it can help with my risk considerations. I can add more possible factors and data protection measures with the help of others. In the short term, it may be okay, but in the long term, it's insufficient. The reason is as mentioned before. Firstly, the private sector needs to survive, and implementing these measures requires resources, which is a practical concern. Additionally, without government policies or incentives, it may not be financially viable for companies to invest in these measures on their own. Evaluating the effectiveness of such investments is not easy, and companies may need to commit significant resources, which might not be cost-effective in the long run. Therefore, in the long term, companies may not be willing to undertake such efforts.

00:37:50 TPR3

This is the first point, and of course, the second one is from the government's perspective, their intention is good, but they also need to invest a lot of resources in this matter. If there is no proactive initiative, meaning that private and government sectors collaborate. I unconditionally share information, wit you and you are also willing to inform me without condition when incidents occur, then we can establish a mutual trust relationship. Only with this trust relationship can we maximize the benefits of such collaboration. Otherwise, it is difficult to achieve success in the long term.

00:38:25 Interviewer

This is really difficult, very difficult, to be able to fully cooperate with that.

00:38:33 TPR3

Yes, building that trust is difficult, and it's not easy. So, as I mentioned earlier, short-term assistance can be helpful. I may invest a sum of money to achieve short-term goals, and it appears to be working well, allowing me to obtain what I need. However, I cannot continue to invest money indefinitely. Therefore, I definitely hope for a life cycle or a relationship within the supply chain of the industry, where both private and government sectors share information. We can contribute data to the government while also receiving valuable information from them. This trust circle needs to be established to create a meaningful collaboration.

00:38:55 Interviewer

Finally, I would like to ask you one more question. I want to ask if you can share some examples of your company or your previous work experience in collaborating with the public and private sectors.

00:39:09 TPR3

For example, in my previous work, I assisted two government agencies and private companies. One of the public sectors is the supervisory authority for the telecommunications agency, which is responsible for telecommunications and telecommunications networks. And the other is a telecommunications network company. The telecommunications network company not only includes the well-known power companies but also includes network companies, which in turn include things like undersea cables, cable television networks, satellite communications, and any other communication network.

00:39:38 TPR3

So, what I did before was actually covering the entire communication network in Taiwan. My job was to help the government establish the mechanism, how the supervisory authority should establish the mechanism, how private organizations should establish the mechanism, how to communicate and cooperate between the two sides, how to establish a trust circle, and what technology and management rules to use. What is the government's strategy?

00:40:08 Interviewer

OK.

00:40:08 TPR3

So, the specific part that stems from this is that we assisted the government in establishing a regulation called the Cyber Security Management Act. Through administrative orders, all large telecommunications and communication network operators are required to comply with these regulations in their planning and implementation. The government also conducts regular inspections.

00:43:24 Interviewer

OK, yes. Now, the government needs the help of private enterprises to establish regulations. Otherwise, the regulations they establish may not be good and useful. People might think, "How could they establish such regulations?"

00:43:35 TPR3

They are just a paper tiger.

00:43:37 TPR3

People just look at them without intention to take actions.

00:43:42 Interviewer

Okay, I think that's about it. Alright.